Undecidability in Resource Theory: Can You Tell Resource Theories Apart?

Matteo Scandi◉* and Jacopo Surace◉†

ICFO–Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology,
Castelldefels (Barcelona) 08860, Spain

A central question in resource theory is whether one can construct a set of monotones that completely characterize the allowed transitions dictated by a set of free operations. A similar question is whether two distinct sets of free operations generate the same class of transitions. These questions are part of the more general problem of whether it is possible to pass from one characterization of a resource theory to another. In the present Letter, we prove that in the context of quantum resource theories this class of problem is undecidable in general. This is done by proving the undecidability of the membership problem for completely positive trace preserving maps, which subsumes all the other results.

Introduction.—The aim of resource theory is to characterize the possibility of action of an agent who acts under some kind of operational restriction [1]. To this end, one specifies a set of transformations that the agent can freely carry out, and asks general questions about its capabilities when it is assumed that the allowed operations can be composed repeatedly in any arbitrary order.

The paradigmatic example of a resource theory is the one of local operations and classical communication (LOCC) [2]. In this case, two agents who can access two different halves of a shared quantum system are allowed to operate only through local transformations and by sharing classical information between them. It is a nontrivial fact that only by composing operations from the LOCC set, a quantum state can be perfectly teleported from one agent to the other [3].

The example above shows that being able to identify whether a transformation is part of a given resource theory is an issue of practical relevance, which can give quite surprising results. It should be noticed, though, that the membership of the quantum teleportation to the LOCC set is proven by explicitly presenting a protocol to implement it. This kind of proof requires a certain amount of ingenuity and the *ad hoc* constructions used do not help identifying generic members of a set. For this reason, the question of whether there is a general way to certify the membership of a transformation to a set of free operations remains open.

A dual perspective about resource theories is given by focusing on states rather than operations. In this context, one assigns to each system a series of labels that quantify how useful the state is. The paradigmatic example is given by entanglement, the resource for LOCC operations. As a matter of fact, most of the nontrivial protocols that can be carried out within LOCC (among these, the quantum teleportation protocol described above) are possible only by the use of entangled states. For this reason, it is also of

practical importance to assess the value of a state within a resource theory.

The standard approach is to define a set of functions, called monotones, which do not increase under the application of free operations. In this way, one can estimate the resourcefulness of a state by looking at a family of numerical labels.

Hence, there exist two possible natural characterizations of a resource theory: in one case, a description of the allowed operations is provided; in the other, a set of value functions, the monotones, are specified. It is natural then to ask whether there is a constructive way to pass from one description to the other. This is equivalent to asking whether it is possible to pass from the description about the operational capabilities of an agent to the determination of the resourcefulness of a state.

We prove here that both of the problems raised above are undecidable for general resource theories of quantum operations: namely, we prove that there is no algorithm that decides whether a generic transformation is generated by a set of free operations, and we show that this implies that there is no algorithmic means of constructing from a set of free operations a set of monotones describing the same resource theory. It also follows from the undecidability of the membership problem that it is impossible to certify whether a transition is part of a resource theory. Moreover, it is shown that given two sets of free operations it is impossible to tell whether they describe the same set of transitions. These negative results hint at the reason why finding a complete set of monotones is usually a difficult task for many particular resource theories.

Definitions.—In this section we provide the main definitions of the objects treated in the rest of the Letter.

Given a set $\mathcal{S}$ and an associative binary operation on it, the semigroup $\mathcal{S}^*$ is defined as the union of all the finite

compositions of elements from $\mathcal{S}$. In other words, $\mathcal{S}$ is the generating set of $\mathcal{S}^*$.

Definition 1: Resource theory.—Given a set of operations $\mathcal{F}$ which contains the identity, the semigroup $\mathcal{F}^*$ characterizes a resource theory. The elements of $\mathcal{F}^*$ are called free operations.

In the following, we only consider the case in which the elements of $\mathcal{F}$ are completely positive trace preserving maps (CPTP) acting on density operators $\mathcal{D}$ and composing in the usual sense of composition of maps.

Free operations naturally induce a partial order on the state space:

Definition 2: Partial order induced by $\mathcal{F}^*$.—Given a set of free operations $\mathcal{F}^*$ and two states $\rho, \sigma \in \mathcal{D}$, we say that $\sigma \leq_{\mathcal{F}} \rho$, if there exists a $\phi \in \mathcal{F}^*$ such that $\phi(\rho) = \sigma$.

Furthermore, if two states can be transformed into one another through free operations, the two states are indistinguishable to the resource theory. This motivates the following definition.

Definition 3: Quotient space.—Any resource theory naturally induces an equivalence relation on the space of states as

$$\rho \simeq_{\mathcal{F}} \sigma \Leftrightarrow \sigma \leq_{\mathcal{F}} \rho \wedge \rho \leq_{\mathcal{F}} \sigma. \tag{1}$$

The natural space in which the resource theory is defined is $\mathcal{D}/\simeq_{\mathcal{F}}$.

In order to quantify the value of a state, one introduces functions which cannot increase under free operations.

Definition 4: Monotones and compatibility.—A function is called monotone (with respect to a resource theory) when it does not increase under the action of the free operations. Respectively, an operation ϕ is said to be compatible with a set of monotones $\mathcal{M}$ if $\forall f \in \mathcal{M} \, \forall, \, \forall \rho \in \mathcal{D} f(\phi(\rho)) \leq f(\rho)$.

Definition 5: Complete set of monotones.—A set of monotones $\mathcal{M}_{\mathcal{F}}$ is said to be complete (with respect to $\mathcal{F}^*$) if

$$\forall f \in \mathcal{M}_{\mathcal{F}}, \ \forall \rho, \quad \sigma \in \mathcal{D}, \quad f(\sigma) \leq f(\rho) \Leftrightarrow \sigma \leq_{\mathcal{F}} \rho. \tag{2}$$

That is, $\mathcal{M}_{\mathcal{F}}$ and $\mathcal{F}^*$ identify the same partial order structure on $\mathcal{D}$.

Main results.—In this section we prove that deciding whether a transition is present in a resource theory is undecidable (Corollary 1), which implies that one cannot tell whether two resource theories presented in terms of free operations are the same (Corollary 2). Moreover, we also show that it is impossible to algorithmically construct from a set of free operations $\mathcal{F}^*$ a set of monotones $\mathcal{M}$ which describes the same resource theory (Corollary 3). These facts are all consequences of the following:

Theorem 1.—The membership problem for semigroups of CPTP maps is undecidable.

Proof.—The main arguments of the proof are inspired by [4,5]. Define two generic matrices in SU(2):
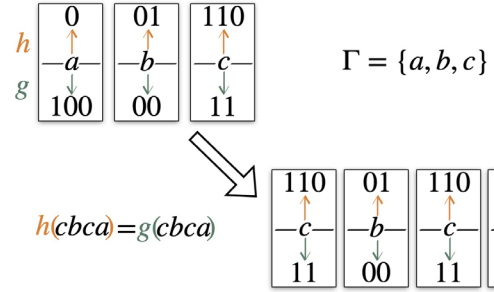

FIG. 1. The PCP can be expressed in terms of dominoes: given the two homomorphisms h and g from Γ^* to $\{0, 1\}^*$, we assign to each letter $x \in \Gamma$ a tile which has in the upper half $h(x)$ written out, and in the lower half $g(x)$. In the example above, $h(a) = 0$ and $g(a) = 100$, so that the a domino is constructed accordingly. Since h is a homomorphism [i.e., $h(xy) = h(x)h(y)$], words in Γ^* can be represented by juxtaposing the dominoes corresponding to each letter in the word. The PCP problem then translates to the question whether one can find a sequence of dominoes that makes the binary word appearing on top equal to the one on the bottom.

$$A = e^{i\theta\vec{n}\cdot\vec{\sigma}}, \qquad B = e^{i\theta\vec{m}\cdot\vec{\sigma}}, \tag{3}$$

where $\vec{n}$ and $\vec{m}$ are vectors in $\mathbb{R}^3$ and $\vec{\sigma} := \{\sigma_x, \sigma_y, \sigma_z\}$ is a vector of Pauli matrices. It was proven in [6] that any pair $\{A, B\}$ of this form generates a free semigroup whenever $\vec{n} \cdot \vec{m} = 0$ and $\cos\theta \in \mathbb{Q}\backslash\{0, \pm 1, \pm\frac{1}{2}\}$. A semigroup of two elements is called free if there is a bijection between its elements and binary strings or, equivalently, if there is no finite composition of its elements that gives the identity. We can then use the two matrices above to encode words in $\{0, 1\}^*$, where the star indicates arbitrary finite juxtaposition of the letters in a given set. Define γ as the homomorphism that assigns to each binary word the corresponding element in the semigroup $\{A, B\}^*$. In other words, γ operates on binary strings by substituting to each 0 an A and to each 1 a B, and the juxtaposition of letters is mapped to matrix multiplication [e.g., $\gamma(010) = ABA$].

In order to prove the theorem we use a reduction to the Post correspondence problem (PCP). Given two different homomorphisms h and g from the finite alphabet Γ to $\{0, 1\}^*$, this is the problem of deciding whether there is a nonempty word $w \in \Gamma^*$ such that $h(w) = g(w)$. This is exemplified in Fig. 1. It is a classical result from computability theory that the PCP is undecidable [7,8]. The idea of the proof is to show that if the statement of the theorem were decidable, then the PCP would be as well, generating a contradiction.

First, for each letter $a_i \in \Gamma$ define the two unitary matrices:

$$h_{a_i} = \begin{pmatrix} \gamma[h(a_i)] & 0_2 \\ 0_2 & A^i B \end{pmatrix}, \tag{4}$$

$$g_{a_i} = \begin{pmatrix} \gamma(g(a_i))^\dagger & 0_2 \\ 0_2 & B^\dagger(A^i)^\dagger \end{pmatrix}. \tag{5}$$

Since both γ and h are homomorphisms, the matrices h_{a_i} compose as $h_{a_i}h_{a_j} = h_{a_ia_j}$ (similarly for g_{a_i}). These matrices are constructed in such a way that the first diagonal block encodes the image of the letter a_i under the homomorphism, while the bottom half is used to keep track of its index.

We can then study the resource theory generated by the set $\mathcal{F} := \{\mathbb{1}, H^\lambda_{a_i}, G^\lambda_{a_i}\}_{a_i \in \Gamma, \lambda \in (0,1)}$, where we defined the following two families of maps:

$$H^\lambda_{a_i}(\rho) := \lambda h_{a_i}\rho h^\dagger_{a_i} + (1-\lambda)\frac{\mathbb{1}}{4},$$

$$G^\lambda_{a_i}(\rho) := \lambda g_{a_i}\rho g^\dagger_{a_i} + (1-\lambda)\frac{\mathbb{1}}{4}. \quad (6)$$

The composition in this case behaves as $H^{\lambda_1}_{a_i}H^{\lambda_2}_{a_j} = H^{\lambda_1\lambda_2}_{a_i a_j}$, and similarly with $G^\lambda_{a_i}$. In this way, one can encode words from Γ^* into operations in $\mathcal{F}^*$ constructed by composing either only $H^\lambda_{a_i}$s or $G^\lambda_{a_i}$s.

We are now ready to prove the claim. Consider the operation

$$\psi(\rho) := \lambda\rho + (1-\lambda)\frac{\mathbb{1}}{4}. \quad (7)$$

Deciding whether $\psi \in \mathcal{F}^*$ is equivalent to the PCP. In fact, the composition rule of the elements in Eq. (6) implies that in order for ψ to be part of the semigroup, there has to be a sequence of h_{a_i} and g_{a_i} that gives the identity. Since the semigroup generated by A and B is free, the only way to obtain the identity in the second diagonal block is by having a composition of the form $g_{a_n}, \ldots, g_{a_2}g_{a_1}h_{a_1}h_{a_2}, \ldots, h_{a_n}$ (or any cyclic composition thereof). At the same time, given that the h matrices and the g matrices cluster in two different groups, in order to get the identity in the first diagonal block the following should hold:

$$\gamma(g(a_n))^\dagger, \ldots, \gamma(g(a_1))^\dagger\gamma(h(a_1)), \ldots, \gamma(h(a_n)) = \mathbb{1}_2, \quad (8)$$

which is equivalent, thanks again to the freeness condition, to the existence of a word $w \in \Gamma^*$ such that $h(w) = g(w)$. This reduces the PCP to the membership problem for CPTP maps. ∎

The theorem just proved has a number of implications. In particular:

Corollary 1: Reachability problem.—Given two states ρ and σ and the description of $\mathcal{F}$, it is undecidable whether there exists $\phi \in \mathcal{F}^*$ such that $\phi(\rho) = \sigma$.

Proof.—This follows directly from the proof of Theorem 1: choose an arbitrary ρ and set σ to be $\psi(\rho)$ [i.e., the state defined by the right hand side of Eq. (7)]. Because of the structure of the semigroup $\mathcal{F}^*$, a transition between the two states is possible if and only if $\psi \in \mathcal{F}^*$. Since this is undecidable, the corollary follows. ∎
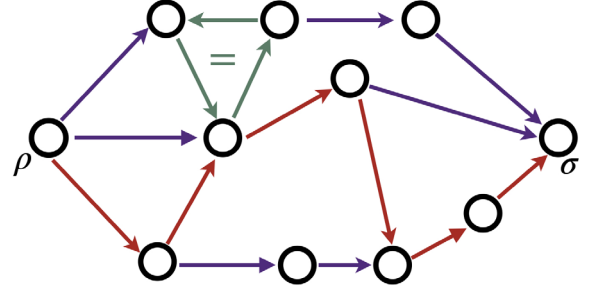
Moreover, it is also easy to see that

FIG. 2. Graphical representation of the action of a resource theory $\mathcal{F}^*$ on the state ρ. Each vertex represents a state, and the presence of an edge from the vertex ρ_1 to ρ_2 corresponds to the existence of a transformation $\phi \in \mathcal{F}^*$ such that $\phi(\rho_1) = \rho_2$. It should be noticed that in order to keep the graph clean, we omitted many edges in the figure. For example, there should be a line directly connecting ρ to σ, since $\mathcal{F}^*$ contains all the compositions. The green arrows show that equivalent states appear in the graph in the form of a cycle. Collapsing all the cycles to a representative vertex makes the graph acyclic. The red line is the longest trajectory between ρ and σ, so that $f^\mathcal{F}_\rho(\sigma) = \frac{1}{7}$.

Corollary 2.—Given two generating sets $\mathcal{F}_1$ and $\mathcal{F}_2$, there is no algorithmic means of deciding whether they describe the same resource theory.

Proof.—Take as $\mathcal{F}_1$ the set $\mathcal{F}$ defined in Theorem 1 and as $\mathcal{F}_2 := \mathcal{F} \cup \{\psi\}$. The transition $\rho \to \psi(\rho)$ is trivially present in $\mathcal{F}_2$. From Corollary 1, though, it is undecidable to say whether this transition is generated by $\mathcal{F}_1$. Hence, deciding whether two different sets of free operations describe the same set of transitions is impossible in general. ∎

Before passing to prove Corollary 3, we present the following:

Lemma 1.—For any $\mathcal{F}^*$ there exists a complete set of monotones.

Proof.—It is natural to first define a set of monotones $\mathcal{M}$ on the quotient space $\mathcal{D}/\simeq_\mathcal{F}$ and to just later extend it to the whole space of density matrices.

The idea of the proof is to assign to each state $\rho \in \mathcal{D}$ a directed graph corresponding to all the possible states reachable from ρ through arbitrary applications of elements of $\mathcal{F}^*$. A graphical depiction of how this looks is presented in the first panel of Fig. 2. Each vertex in the figure corresponds to a state, and the presence of an arrow from the vertex ρ_1 to ρ_2 corresponds to the existence of a transformation $\phi \in \mathcal{F}^*$ such that $\phi(\rho_1) = \rho_2$. Passing from $\mathcal{D}$ to the quotient space $\mathcal{D}/\simeq_\mathcal{F}$ makes the graph acyclic, since all the vertices in the same equivalence class (like the ones connected by the green lines in the figure) collapse to a single point.

In order to define monotones on $\mathcal{D}/\simeq_\mathcal{F}$, we then only have to focus on acyclic directed graphs. Moreover, one has to assign to each continuous semigroup $\{\Phi_t\}_{t \in \mathbb{R}} \subset \mathcal{F}^*$ a generator $\mathcal{L}$, i.e., a map satisfying $\Phi_t =: e^{t\mathcal{L}}$. At this point, a length can be assigned to each edge in the graph: if the

transformation corresponding to an edge cannot be further decomposed inside $\mathcal{F}^*$, then we assign a length one; if the transformation is part of a semigroup generated by a single element $\mathcal{L}$, the length is given by the parameter t; finally, if an edge corresponds to multiple transformations, the length is inductively defined as the sum of the lengths. We can then assign to each state $\rho \in \mathcal{D}_C$ a monotone $f_\rho^{\mathcal{F}}$ in the following way: (i) if a state σ cannot be reached from ρ, then $f_\rho^{\mathcal{F}}(\sigma) := 2$; (ii) if σ is part of at least one of the trajectories stemming from ρ, then assign the value $f_\rho^{\mathcal{F}}(\sigma) := [1/(\ell + 1)]$, where ℓ is the length of the longest path from ρ to σ. Finally, $f_\rho^{\mathcal{F}}$ can be extended to the whole space of density matrices, by assigning to two representative of the same equivalence class $\sigma_1 \simeq_{\mathcal{F}} \sigma_2$ the same value, $f_\rho^{\mathcal{F}}(\sigma_1) \equiv f_\rho^{\mathcal{F}}(\sigma_2)$.

In order to prove that the set $\mathcal{M} = \{f_\rho^{\mathcal{F}}\}_{\rho \in \mathcal{D}}$ is complete, we first need to prove that it is compatible. This holds by construction. In fact, suppose that there exists a $f_\rho^{\mathcal{F}}$, a σ, and a $\phi \in \mathcal{F}^*$ such that $f_\rho^{\mathcal{F}}(\phi(\sigma)) > f_\rho^{\mathcal{F}}(\sigma) := [1/(s+1)]$. The longest trajectory from ρ to $\phi(\sigma)$ is long at least $s + \varepsilon$ for some positive ε, implying that $f_\rho^{\mathcal{F}}(\phi(\sigma)) \leq [1/(s+\varepsilon+1)] < [1/(s+1)]$, which gives the desired contradiction. Similarly, it also follows by construction that the set is complete. Assume that for two given states ρ and σ and $\forall f \in \mathcal{M}$ one has $f(\sigma) \leq f(\rho)$. This directly implies that $f_\rho^{\mathcal{F}}(\sigma) \leq f_\rho^{\mathcal{F}}(\rho) = 1$, so by definition there exists a trajectory from ρ to σ or, in other words, a $\phi \in \mathcal{F}^*$ such that $\phi(\rho) = \sigma$. This concludes the proof. ∎

Lemma 1 shows that monotones can be as powerful in constraining a resource theory as the usual characterization in terms of free operations. Since we are just interested about the possibility in principle, we constructed an overcomplete set $\mathcal{M}$, setting aside questions about finding the minimal complete set. It is worth pointing out, though, that in many resource theories the complete set is actually finite: for example, in the resource theory of nonuniformity one only needs $d - 1$ monotones, where d is the dimensionality of the Hilbert space [9]. Before investigating how one could find a minimal complete set, it is important to understand whether such a complete set could be found at all. The negative answer to this issue is given by the following:

Corollary 3.—Given a set of free operations $\mathcal{F}$ there is no algorithmic means of constructing a recursive complete set of monotones $\mathcal{M}$ associated with it.

Proof.—Lemma 1 implies the existence of a complete set of monotones $\mathcal{M}$ associated to $\mathcal{F}$. Assume the existence of an algorithm constructing this set. Moreover, also assume the existence of an algorithm $\mathcal{A}_{\text{cmp}}$ which takes two arbitrary states ρ and σ as input, and decides whether $\forall f \in \mathcal{M}, f(\rho) \geq f(\sigma)$. If such an algorithm did not exist, then the claim would follow trivially, since one wouldn't be able to check the compatibility of $\mathcal{F}$ with $\mathcal{M}$. If such an algorithm existed, then one could decide whether a transition between two arbitrary states is present in $\mathcal{F}^*$ simply

by running $\mathcal{A}_{\text{cmp}}$. This is in contradiction with Corollary 1. Therefore, there is no general algorithm constructing the complete set $\mathcal{M}$ associated with $\mathcal{F}$. ∎

Conclusions.—In the present Letter, we showed that standard questions in resource theories hide undecidability issues. Consider, for example, the main problem in this context: whether it is possible to convert a state into another through a series of allowed operations. The undecidability of this question is the content of Corollary 1. This directly implies the impossibility of completely identifying a generic resource theory. In particular, given two different characterizations of a resource theory in terms of two different sets of free operations, it is impossible to tell whether they induce the same set of transitions (Corollary 2). Finally, Corollary 3 implies that it is also impossible to construct a set of value functions which completely describes the resource theory induced by a set of free operations.

The main theorem supporting these results is the undecidability of the membership problem for semigroups of CPTP maps (Theorem 1). It should be noticed that in the proof of this theorem we used a resource theory which, if somewhat artificial, has anyway a precise physical interpretation: the maps $H_{a_i}^\lambda$ and $G_{a_i}^\lambda$ defined in Eq. (6) are rotated depolarising channels, which correspond to the experimental setting in which one can only apply unitary transformations of the form h_{a_i} or g_{a_i}, introducing at each application some quantum noise into the system.

Nonetheless, it would be interesting to prove the same theorem within the framework of a more natural resource theory. A promising candidate in this respect is given by the LOCC set: its structure is notoriously difficult to characterize mathematically [10], a fact that could be explained if one could show that it contains an undecidable set. This challenging possibility would require the devise of a new proof and it is left for future research.

[*]Matteo.Scandi@icfo.eu
[†]Jacopo.Surace@icfo.eu

[1] E. Chitambar and G. Gour, Quantum resource theories, Rev. Mod. Phys. **91**, 025001 (2019).

[2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81,** 865 (2009).

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an Unknown Quantum State Via Dual Classical and Einstein-Podolsky-Rosen Channels, Phys. Rev. Lett. **70,** 1895 (1993).

[4] P. Bell and I. Potapov, On the membership of invertible diagonal and scalar matrices, Theor. Comput. Sci. **372,** 37 (2007).

[5] P. Bell and I. Potapov, Reachability problems in quaternion matrix and rotation semigroups, Inf. Comput. **206,** 1353 (2008).

[6] S. Świerczkowski, A class of free rotation groups, Indagat. Math **5,** 221 (1994).

[7] E. L. Post, A variant of a recursively unsolvable problem, Bull. Am. Math. Soc. **52,** 264 (1946).

[8] M. Sipser, *Introduction to the Theory of Computation* (Cengage Learning, Boston, 2012).

[9] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Yunger Halpern, The resource theory of informational nonequilibrium in thermodynamics, Phys. Rep. **583,** 1 (2015).

[10] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, Everything you always wanted to know about LOCC (but were afraid to ask), Commun. Math. Phys. **328,** 303 (2014).

[11] M. M. Wolf, T. S. Cubitt, and D. Perez-Garcia, Are problems in Quantum Information Theory (un)decidable? arXiv:1111.5425.